Sonr: A P2P Identity Verification System - Draft 1

Prad Nukala

May 26, 2023

Abstract

Existing mechanisms for user identity with their lack of standardization have led to faulty solutions that source information from closed third-party sources. By introducing a new peer-to-peer network we solve this issue at the point of the device and leverage a blockchain system to verify User claims. Sonr provides the utility of managing crypto assets, private identifiable information, and application specific data while having full W3C Decentralized Identifier compliance.

Warning: The contents of this document are subject to change from the time being until the launch of our public network. We are providing this as an in-depth analysis for our current stakeholders. A more finalized version of this whitepaper will be distributed prior to network launch.

1 Introduction

Sonr is a Cosmos powered blockchain which is powered by a TenderMint validation mechanism. The default consensus for TenderMint is DPoS and works with our current ABCI implementation for Transaction Verification. DPoS is a twist on Proof of Stake consensus that relies upon a group of delegates to validate blocks on behalf of all nodes in the network . Witnesses are elected by stakeholders at a rate of one vote per share per witness . Coin age is irrelevant. All coins that are mature will add the same staking weight (usually 1 in the wallet hover display) Results in stable, consistent interest only for active wallets and only with small inputs.

1.1 Delegated Proof of Stake (DPoS)

On Sonr we will be leveraging a delegate stake mechanism in order to optimize buy-in for users in the network. It imposes an excess opportunity cost if slashing is implemented.

With this being said, there are some challenges in implementing staking:

- The token must already have value
- Allocating power or influence via staking gives major edge to wealthy users
- They are frequently subject to gaming and coordination problems

However there is substantial benefit in incorporating a staking mechanism, with the following criteria met we can create a sustainable design:

1. The upfront capital required to stake should not significantly discourage them to stake
2. If a stakeholder group is making decisions that materially harm the network, they would be punished via slashing the stake.
3. Stakeholders can make decisions that positively impact the future network health and token price, therefore holding stake can promote positive Sonr growth

2 Decentralized Identity

Sonr's x/identity is a decentralized identity and asset management module that uses MPC Wallet Generation, DID Resolution, and Interchain Accounts to provide users with secure, user-friendly control over their data.

2.1 Identity Keyshare System

Sonr's system leverages the powerful cryptographic technique of Multi-Party Computation (MPC) for secure wallet generation and DID (Decentralized Identifier) resolution. As part of this process, keyshares are generated which form an integral part of the MPC technique.

2.2 Multi-Party Computation (MPC)

In MPC, a secret value (in this case, a user's private key) is divided into a number of shares. These keyshares are such that any subset of them can be used to reconstruct the secret, but no single share reveals any information about the secret itself. This ensures that even if a malicious party gains access to a share, they can't derive any meaningful information about the private key.

2.3 Encrypted Decentralized Storage

The security and confidentiality of these keyshares are of paramount importance for the system's security. To ensure this, Sonr stores these keyshares in encrypted IPFS vaults. IPFS, or InterPlanetary File System, is a decentralized storage solution. Unlike traditional file storage systems, where files are located at specific server locations, IPFS identifies files based on their content, making it a robust and resilient system for storing information.

When a keyshare is generated in Sonr's system, it is encrypted and stored in an IPFS vault. This vault is then "pinned," meaning it is marked for preservation and can be retrieved reliably from the IPFS network. This approach combines the benefits of MPC's secure computation with IPFS's resilient storage to create a robust security model for managing digital identities and wallets.

3 Application Services

The x/service Module of Sonr's system plays a crucial role in managing and authenticating user interactions with the network. It provides several key functionalities, including WebAuthn-based user authentication, Service Record management and registration, and DNS resolution and record verification.

3.1 DNS Record Verification

The most basic cryptographic mechanism employed by Sonr is for TXT record verification of origin urls. In order for a service to have the ability to engage with the Sonr network the client needs to deploy a Service Record with a valid, resolvable origin url. The validator node provides the client with a challenge in order to verify ownership of the domain and to insert as a record on their domains DNS routing table. This mechanism is subject to change, as the Sonr core team look's for a more scaleable, decentralized approach.

3.2 Verifiable Random User Assertion

A VRF operates like a regular hash function, but with an added feature: it provides a proof of the randomness. This proof ensures that the random number was generated by the specific private key holder and could not have been tampered with or predicted in advance.

When a user requests assertion options from a validator node in the Sonr network, the VRF is employed to generate a challenge. This challenge is unique, unpredictable, and cannot be precomputed or reused. The output from the VRF is used to create the challenge, and a corresponding proof is generated.

The proof and the challenge are then sent back to the user. The user verifies the proof against the validator's known public key before continuing. This way, the user can be assured that the challenge was created freshly by the validator and has not been tampered with during transit.

The challenge is kept private, providing privacy to the user's authentication activity. Simultaneously, the deterministic nature of the VRF ensures that any disputes can be resolved, as anyone can use the proof and the validator's public key to confirm the challenge's correctness.

4 Vault Storage

The x/vault Module is a private module which manages the encryption, storage, and retrieval of sensitive data in the Sonr network.

4.1 Incorporation of WebAuthn

WebAuthn is a web standard published by the World Wide Web Consortium (W3C) for strong user authentication. It's typically used to replace or supplement password-based authentication with public key cryptography, providing a way for users to prove their identity to a service without transmitting a shared secret over the network.

However, in our system, we use WebAuthn for a different purpose: secure key storage and encryption. Specifically, we use the public-private key pair associated with a WebAuthn credential as the basis for an encryption scheme, with the private key securely stored on the user's device and the public key stored on the Authentication field of the User's DID Document.

In the context of Sonr, the data that WebAuthn encrypts is the associated Multi-Party Computation (MPC) shard for the device. The MPC shard, a piece of data crucial for the operation of our system, must be kept private and secure. By using WebAuthn for encryption, we can ensure that the MPC shard is only accessible to the legitimate owner of the device. When linking a new device, we regenerate the pool of MPC shares and add an additional share to be mapped for the new Device credential.

4.2 ECIES Asymmetric Encryption

ECIES (Elliptic Curve Integrated Encryption Scheme) is a cryptographic protocol that uses elliptic curve cryptography to secure data transmission. It allows a sender to encrypt a message using the recipient's public key in a way that ensures only the recipient, who possesses the corresponding private key, can decrypt and access the message, thereby providing confidentiality in message exchange.

To achieve encryption, we employ an Elliptic Curve Integrated Encryption Scheme (ECIES). In this process, we first convert the public key from the WebAuthn credential from 'webauthncose.EC2PublicKeyData' format to 'ecdsa.PublicKey' format.

Following this, we generate an ephemeral key pair and derive a shared secret from the ephemeral private key and the public key. Using the derived shared secret, we then derive encryption and MAC (Message Authentication Code) keys.

The MPC shard is then encrypted with AES-256-GCM using the derived encryption key and a randomly generated IV (Initialization Vector). A MAC tag is also computed to ensure the integrity of the 'ciphertext'.

The final output of this process is a single byte slice that concatenates the encoded ephemeral public key, the IV, the 'ciphertext', and the MAC tag. This byte slice is then stored securely on the IPFS Network.

4.3 NACL Secret Box

In the context of Sonr, the sender encrypts the message using the recipient's public key and their own private key. The encrypted message can then be safely sent across the network, secure in the knowledge that only the recipient, with their corresponding private key, can decrypt it. The NaCl secret box is used for encrypting and decrypting messages. The 'secret box' construct in NaCl provides authenticated encryption. This means that data is not only kept confidential, but also that any tampering with the data can be detected.

4.4 Sonr File System (SFS)

The SFS is a distributed file system that provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks. This forms the basis for a decentralized version of a traditional hierarchical file system.

A KDF, such as PBKDF2 or HKDF, takes an input (or 'password') and produces a derived key. By inputting different parameters for each use case, we can produce distinct keys for each application.

This ensures that a compromise in one area, such as a user's inbox messages, would not lead to a compromise in another, such as their MPC shards.

Within the SFS, user data such as inbox messages, push notifications, and MPC shards are stored in an encrypted form. Only the user, with their derived keys, can access and decrypt their own data.

5 Incentive Structure

In order to maximize buy-in and network availability for the Sonr ecosystem, we will be implementing an empirical Token Rewards mechanism. Rewards are a way to create inflation in order to dilute the token value, resulting in an affordable onboarding and operational experience for the end user. The goal behind Sonr Token rewards is to subsidize Highway based computation, in order to promote value creation and platform growth.

5.1 IPFS Storage Replication

When deploying standalone highway nodes, requiring minimum stake would be an additional method to enforce availability requirements. By having a stake we can ensure that the user deploying a node has a base level of buy-in within the ecosystem.

5.2 MPC Account Generation

The generative account incentive model works by having a validator generate a new account and place it in an unclaimed accounts list. When a user requests a new account, they are given the creation options for the oldest unclaimed account. The user then generates a WebAuthn credential and submits it to the Highway. The Highway verifies the challenge and broadcasts the DID document to the blockchain. The user is then given a success message. The generative account incentive model creates a predictable flow of token minting which fluctuates based off Network ingress. Aside from this our model offers a number of benefits over traditional account creation methods, including:

- Increased security - MPC ensures that user accounts are secure and that user data is private.
- Improved privacy - WebAuthn allows users to create accounts without revealing their personal information.
- Reduced costs - The generative account incentive model eliminates the need for expensive hardware and software solutions.

6 Governance Participation

At the time of Main-net launch, phase one of the Sonr governance rollout will be implemented and will result in a set of rewards for participants.

6.1 Submission of Proposals

Users will be incentivized to submit blockchain improvement or grant proposals to be reviewed by voting participants. In order to prevent game from low quality and out of scope proposals, a clear-cut submission and evaluation process will be put into place on a public facing FAQ website.

6.2 Proposal Voting

In order to prevent innovation from halting on the Sonr ecosystem, we incentivize all staked users to participate in the polling process for community submitted proposals. Users are then rewarded for good-faith participation in voting, while also sustaining momentum.